United States Department of the Interior

BUREAU OF LAND MANAGEMENT
Montana State Office
5001 Southgate Drive, P.O. Box 36800
In Reply To: Billings, Montana 59107-6800
http://www.mt.blm.gov/

1264 (932.NS) P March 1, 2004

EMS TRANSMISSION – 3/1/04
Instruction Memorandum No. 2004-035
Expires: 9/30/05

To: State Management Team

From: State Director

Subject: Requesting Computer Access for New Users and Initial Security Requirements

Program Area: Information Technology (IT) Security

Purpose: This memorandum explains the process by which supervisors will obtain Windows domain (PC) and email accounts for a new user. The term new user applies to volunteers, contract workers, new employees, other agency cooperators and any user who is being authorized access to the BLM system.

Policy/Action:

Documentation Required (2 Forms)

A. Form 1264-3 "Individual Computer User's Statement of Responsibility." This document must contain the signature of the new user. (The cover page with the title "General Rules and Guidelines Governing the Use of BLM Computer Systems" should be read and retained by the user.)

1. New employees are sent this form along with their employment confirmation letter with instructions to return it to Human Resources. Human Resources send a copy to the IT Security Manager.

2. Volunteers, contract workers, and any other cooperators who are authorized access to use our system are given or sent this form by the local office for signature. The local office is responsible for forwarding it to the State IT Security Manager for retention. (The only exception to this rule is if the volunteer already has a 1264-3 on file due to past employment/volunteer service with Montana/Dakotas BLM.) If an office does not have this form, please contact Human Resources at the Montana State Office.

B. Montana Form 1264-1 "Montana New User Access Request Form." This form can be found at mtso03/blm.share/records/forms/MT-1264-1.doc and asks for information about the new user including a check list for the application this user needs to access. If applications are checked, the IT Security Manager will inform the appropriate application contacts. The contact for the application will explain the process to the new user. An example of the MT-1264-1 is attached.

Creating an Account Before the Employee's Reporting Date:

Accounts may be created before the new user's reporting date. The State IT Security Manager must receive the following documentation a minimum of one business day prior to establishing the new accounts.

1) The 1264-3 form: For new employees the form will be sent to them with their confirmation letter. For others, the supervisor should see that a 1264-3 is sent and returned and on file with the IT Security Manager before requesting an account to be created.

2) The MT-1264-1 form: The form should contain the supervisor's signature which authorizes the early creation of these accounts.

The creation of the PC account will be performed by the respective Zone System Administrator for the field office unless he/she is unavailable. In that case it will be created by Montana State Office personnel. Those creating the accounts will contact the State IT Security Manager to verify that the paperwork is in place and to inform the IT Security Manager that the account has been created and disabled.

Though created before hand, these accounts will not be enabled until the new user is physically present in the local office. At that time, the local office will contact either the Montana Help Desk or the Zone System Administrator who will enable the accounts.

Creating an Account Upon the Employee's Physical Presence in the Office:

Sometimes someone needing access arrives in the office before accounts are requested. In that case the following should be completed.

1) The MT-1264-1 form: This form can be e-mailed/faxed to the Montana Help Desk by the supervisor to ensure that it is processed expeditiously. The e-mail or fax will be forwarded to the State IT Security Manager for retention.

2) The 1264-3 form: The form must be on file with the State IT Security Manager within two weeks of the creation of any account. If it is not, the account may be disabled until the form is on file.

Accounts will be created within 1 business day of receiving this request. The creation of the PC account will be performed by the respective Zone System Administrator for the field office unless he/she is unavailable. In that case it will be created by Montana State Office personnel. Those creating the accounts will contact the State IT Security Manager to verify this has been completed

All New Users

Changing Passwords: The first time a new user logs in they must be accompanied by someone (e.g. supervisor, system administrator) who will ensure that the new user changes the password on both the PC and e-mail accounts. This ensures that no accounts are left open with a default password.

What Every Employee Should Know: In addition, all new users should be introduced to the "What Every Employee Should Know" link on the Montana/Dakotas intranet home page (http://web.mt.blm.gov/empweb/index.html).

This site lists user responsibilities for such things as desktops, laptops, security, and the reporting of security incidents and a link called "Contacts for Access to Applications."

Mandatory IT Security Training: The site also contains a link to the mandatory on-line Security Training that must be completed within two weeks of initial computer access. After completing training, the new user should print and send the certificate of completion to the State IT Security Manager. A photo copy is acceptable.

Budget Impact: Minimal

Background: The BLM's networked systems consists of thousands of personal computers, workstations, remote access, and a variety of servers linked together using numerous technologies. These networks provide connectivity to all BLM sites to facilitate the processing of BLM's mission-dependent information. Data, including sensitive and Privacy Act information, resides on and passes through the components of BLM's networks. Appropriate safeguards must be implemented to control access to IT systems and applications. The BLM's distributed IT systems require the cooperation of BLM users and contract personnel throughout the organization to ensure that access to IT systems and applications are properly controlled.

Manual/Handbook Sections Affected: This process is in line with the directives contained within the BLM IT Security Handbook H-1264-1.

Contact: Please direct your questions to Norma Smith, State IT Security Manager; Asko Virtanen, Alternate State IT Security Manager; or Robin Stoebe, State Chief Information Officer, at 406-896-5270.

Signed by: A. Jerry Meredith, Associate

Authenticated by: Laura Schmier (MT-932)

Distribution
Assistant Field Manager, Glasgow Field Station
Assistant Field Manager, Havre Field Station
AOs